Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/130105

Improved Certificateless Signcryption for IoT Smart Devices

Balasubramanian V.[1,*] *and Mala T.* [2]

[1] Department of Computer Science and Engineering, SSN College of Engineering, Chennai, India
[2] Department of Information Science and Technology, College of Engineering, Anna University, Chennai, India

Received: 18 Mar. 2018, Revised: 12 Aug. 2018, Accepted: 19 Aug. 2018
Published online: 1 Jan. 2019

Abstract: Signcryption achieves both encryption and digital signature at the same time. The cost of the computations involved and the overheads involved in the communication is smaller than the conventional sign-then-encrypt method. Certificateless cryptosystem intends to solve the disadvantage of the identity-based cryptosystem: key escrow problem. It also simplifies the public key management. In this paper, an enhanced new certificateless signcryption technique is proposed by employing bilinear pairings. The scheme performance is also demonstrated to be more effective and efficient for smart devices. The proposed scheme fulfills public ciphertext verifiability and satisfies indistinguishability against adaptively-chosen ciphertext attacks. It is also immune to existential unforgeable against chosen message attacks.

Keywords: Certificateless Signcryption, Bilinear Pairing, Standard model

1 Introduction

The modern cryptography started with the implementation of public key cryptography (PKC). With regards to PKC, each user has a pair of keys (private key, public key). The private key is used for digital signature of a message. The corresponding public key is employed for encryption and for verification of the signature. On the way to confirm whether a public key belongs to the correct identified user, the public key is related to a certificate specified by a Certificate Authority (CA). It is part of the Public Key Infrastructure (PKI). CA is responsible for providing, retaining and invalidating and revoking a large number of certificates. This necessitates a lot of resources when installing in the real scenario.

The chance of identity-based cryptography was proposed in [1] and its intention is to overcome certification of the public keys, a drawback in PKI settings. Here, the public key of each member is acquired from their public identity. The identity can be as an email address, IP address, user name, etc., which is able to distinguish the member. In ID-based cryptosystem, the public key might be any string or it can be derived from any string. To implement this, it needs the existence of a Private Key Generator (PKG), which is a trustworthy authority. The PKG produces users' private key from the user identity information. Identity-based cryptosystem was first constructed practically and described in [2] and it made use of the properties of bilinear maps. The identity-based signcryption scheme was first demonstrated in [3] along with its security model. It is an extension of identity-based encryption to signcryption.

As discussed earlier, to avoid certificates, certificateless cryptography is introduced and described in [4]. Here, the certificate was not needed, and also the PKG could not get the user private key. The reason is, the key is calculated by both the PKG and the user such that user only obtains the result. The part which is still given by the PKG is processed from a master secret key and the users' identity. We now investigate the issue of certificateless signature (CLS) schemes and related work before elaborating our contribution on this area.

Confidentiality, Integrity, authentication, and non-repudiation are the security necessities in cryptographic protocols. Encryption is used to accomplish confidentiality. The extra stated attributes are attained by digital signatures. To meet all these attributes at the same time, the effective way is encrypting and signing separately. A signcryption scheme is a cryptographic technique that achieves all the security

* Corresponding author e-mail: balasubramanianv@ssn.edu.in

requirements simultaneously [5]. The signcryption should possess the attributes like Correctness: technique should be provable; efficient and secure: it should fulfill the security requirements simultaneously. It should provide encryption and digital signature in one go. It can also provide unforgeability and non-repudiation.

The rest of this paper is structured as follows: the certificateless signcryption scheme is described with its formal model and adversarial model is discussed in section II. In section III, the improved scheme is discussed. The improved scheme is analyzed in terms of performance and security is discussed in section IV. In section V, the conclusion and future work are discussed.

2 Preliminaries

A formal model of the Certificateless Signcryption scheme [6] (CLSC) using Bilinear Pairing basics are discussed in this section. It comprises 3 components: a sender - S, a receiver -R and a Key Generation Center(KGC). Its scheme comprises six algorithms:

Bilinear pairing : let n be a prime number. Let $G_1 = \langle P \rangle$ be an additive group of order n. Its identity element is ∞, and let G_T be a multiplicative group of order n. Its identity element is 1.

A *bilinear pairing* on (G_1, G_T) is a map defined as $e : G_1 \times G_1 \rightarrow G_T$ and satisfies the below conditions:

1.Bilinearilty: For all $R, S, T \in G_1$
$e(R+S,T) = e(R,T)\, e(S,T)$
$e(R,S+T) = e(R,S)\, e(R,T)$

2.Non-degenracy:$e(P,P) \neq 1$

3.Computable: e should be easily computable

4.$\forall (S,T) \in G_1$
(a)$e(S,\infty) = 1$ and $e(\infty,S) = 1$
(b)$e(S,-T) = e(-S,T) = e(S,T)^{-1}$
(c)$e(aS,bT) = e(S,T)^{ab}\ \forall (a,b) \in \mathbb{Z}$
(d)$e(S,T) = e(T,S)$

2.1 Definition of Certificateless Signcryption

Certificateless signcryption involves three entities: a key generation center, a sender and a receiver.
It uses six algorithms.

1.*Setup:* It is a randomised algorithm. The Key Generation Centre (KGC) takes security parameter 1^k as input and produces master secret key s and system parameter *Params*. *Params* are made public and KGC keeps s secret.
Setup$(1^k) \rightarrow (Params, s)$

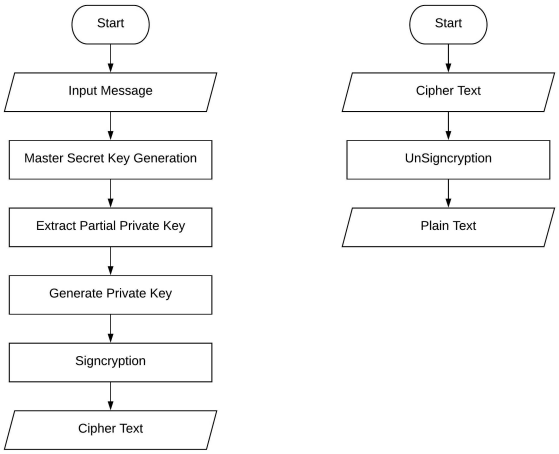

Fig. 1: Flow Diagram of Certificateless Signcryption Scheme

2.*Partial private key generation:* KGC takes *Params* and user identity $ID \in \{0,1\}^*$ as input, along with s and outputs Partial Private Key PSK_{ID}. It is sent to the user.
Partial private key generation $(Params, ID, s) \rightarrow PSK_{ID}$

3.*User key generation: Params* and user identity *ID* is given as input, and the user selects a random secret value x_{ID}, and generates a Public Key PK_{ID}. Certification is not required for the public key.
User key generation $(Params, ID, x_{ID}) \rightarrow PK_{ID}$

4.*Private key generation: Params*, user identity *ID* and secret value x_{ID} are given as input and private key SK_{ID} is generated.
Private key generation $(Params, ID, x_{ID}) \rightarrow SK_{ID}$

5.*Signcryption:* It takes *Params*, identity of sender and receiver ID_s and ID_r, the private key of the sender SK_s, the public key of sender and receiver PK_s and PK_r, message m as inputs and produces cipher text σ
$\sigma = Signcrypt\,(Params, ID_s, SK_s, PK_s, ID_r, PK_r, m)$

6.*UnSigncryption:* It takes *Params*, identity of sender and receiver ID_s and ID_r, the public key of sender and receiver PK_s and PK_r, the receivers' private key receiver SK_r and the cipher text σ, and produces a plaintext m or an invalid symbol $\perp$
$m = UnSigncrypt(Params, ID_r, SK_r, PK_s, ID_s, PK_r, \sigma)$

2.2 Security Notions

Two sorts of adversaries [7] are considered while discussing certificateless public key cryptography. The adversaries are A_I and A_{II}. A_I is an adversary who has the capability to replace the public key of an arbitrary entity. But it does not have access to the master secret key. It is called key replacement attack. A_{II} is an adversary who possesses the master secret key. He cannot replace any public keys. This adversary is a malicious-but-passive KGC [7]. The adversaries try to decrypt a ciphertext or forge a signature. The adversary can obtain information from the environment.

The adversary has access to oracles and requests some information. The two important security requirements of the signcryption scheme are confidentiality and unforgeability. The possible security attacks are adaptive ciphertext attacks (IND-CCA2) and chosen messages attacks (UF-CMA).The system should be immune against these attacks. To present these attacks, it has been defined by a security model with a game between an adversary A and a challenger C. The security notion explained by the game is defined by following oracles.

In the beginning, a setup algorithm is run by the challenger C picking a random number k - security parameter as input and returns the public system parameters. The generated parameters are sent to A on its request. The adversaries have access to these oracles described below:

1. *Setup:* The Challenger C runs the setup algorithm.
   Setup$(1^k) \rightarrow (Params, s)$.
   Params is given to A_I and the challenger C keeps the master secret key s
2. *Find Stage:* A_I can adaptively make a polynomially-bounded number of queries as follows using the oracles:
   (a) *Extract partial private key oracle:* Adversary A gives identity ID as input to C, and C computes the corresponding Partial Private Key PSK_{ID}, and returns to A
   $ExtractPartialprivatekeyoracle_{Challenger}$(ID) $\rightarrow$ PSK_{ID}.

   (b) *Request public key oracle:* Adversary A gives identity ID as input to C, and C computes the corresponding Public Key PK_{ID}, and returns to A
   $Requestpublickeyoracle_{Challenger}(ID) \rightarrow PK_{ID}$.

   (c) *Replace public key oracle:* Adversary A gives identity ID and a new public key PK^1_{ID} to C, and the challenger replaces the current PK_{ID} with the new one PK^1_{ID}.

   (d) *Extract private key oracle:* Adversary A gives identity ID to C, and the challenger computes the corresponding private Key SK_{ID} whose public key is not replaced, and returns it to adversary A
   $Extractprivatekeyoracle_{Challenger}(ID) \rightarrow SK_{ID}$.

   (e) *Signcryption oracle:* A Signcryption oracle takes message m, two identities $\{ID_r, ID_s\}$ from adversary A. Challenger C computes
   σ = *Signcrypt* (SK_s, PK_r, m) and returns σ to adversary A.
   If ID_s public key PK_{ID} has been replaced, then A needs to supply ID_s, secret value x_s to make C compute correct σ.

   (f) *UnSigncryption oracle:* Adversary A supplies two identities $\{ID_r, ID_s\}$ and a cipher text σ. Challenger C computes $UnSigncrypt(SK_r, PK_s, \sigma)$ and returns m or an invalid symbol $\perp$ to A. If ID_s public key PK_{ID} has been replaced, then A needs to supply ID_s, secret value x_s to make C compute unsigncryption.
   The adversary A_I has access to all the above Oracles. The adversary are A_{II} is malicious but passive KGC has access to all the above oracles except *a* and *c*, i.e., *Extract partial private key oracle* and *Replace public key oracle.*
3. *Challenge stage:* Adversary creates two messages of same length $\{m_0, m_1\}$ and two identities $\{ID_r, ID_s\}$. C randomly selects b $\in \{0, 1\}$. Computes
   σ^* = *Signcrypt* $(m_b, SK_s, , PK_r)$
   and sends σ^* to A.

4. *Guess Stage:* Adversary A is allowed to make a polynomial bounded number of queries like in Find Stage(). Adversary A outputs the guess b^1. If b^1 = b, then A wins the game.

A Certificateless Signcryption is said to be secure if it challenges both A_I and A_{II} attacks [8] [9]. We know Type 1 attack is to request and replace public key with a value of its choice using the oracles mentioned above. It does not know the master secret key s. Type II attacker represents malicious PKG who generates a partial private key of users. This attacker knows the master key. It is not able to replace a public key. It is because it can compute the full private key from the partial private key and the user secret key using Extract private key oracle.

Table 1: Scheme

Variables	Description
k	Security Parameter
G_1, G_2	Cyclic Groups
g	Generator of group
e	A bilinear Map $e: G_1 \times G_1 \rightarrow G_T$
s	Master Secret Key
PSK_{ID}	Identity ID's Partial Private Key
PK_{ID}	Identity ID's Public Key
SK_{ID}	Identity ID's Private Key

2.3 Game 1: Confidentiality

A CLSC [10] scheme is said to be indistinguishable - certificateless signcryption against adaptive chosen ciphertext attack property *IND-CLSC-CCA*, if no polynomial bounded adversaries A_I and A_{II} have non-negiligible advantage of winning the game. The game is carried out between a challenger C and adversary A_I.

1. *Initialization:* challenger C runs the *Setup* algorithm and generates a master secret key s and the public system parameter *params*. Challenger C keeps s secret and sends *params* to A_I.
   Setup$(1^k) \rightarrow (Params, s)$

2. *Phase I Queries:*
   Adversary A_I request the oracles with C: *Extract Partial Private Key Oracle, Request Public Key Oracle, Replace Public Key Oracle,Extract Private Key Oracle, Signcryption Oracle*

3. *Challenge stage:*
   Adversary creates two messages of same length $\{m_0, m_1\}$ and two identities $\{ID_r, ID_s\}$. C randomly selects b $\in \{0,1\}$. Computes
   σ^* = *Signcrypt* $(m_b, SK_s, , PK_r)$
   and sends σ^* to A.

4. *Guess stage:* Adversary A is allowed to make a polynomial bounded number of queries like in Find Stage(). Adversary A outputs the guess b^1. If b^1 = b, then A wins the game. The following conditions hold:

   (a) Adversary A_I cannot get private key SK for any identity if his public key has been replaced PK

   (b) Adversary A_I cannot obtain private key SK_{ID_r} for ID_r at any point.

   (c) Adversary A_I cannot obtain partial private key PSK_{ID_r} for ID_r, if the corresponding public key has been replaced already.

   (d) In the guess stage, adversary A_I cannot make an *Unsigncryption* query on σ^* under ID_{r^*}, ID_{s^*}, unless the ID_{r^*}, ID_{s^*} has been replaced after the challenge phase.
   The advantage of A_I is defined as

$$Adv_{A_I}^{IND-CLSC-CCA-1} = \left|2Pr\left|b = b^1\right| - 1\right|$$

A certificateless signcryption scheme(CLSC) is *IND-CLSC-CCA-1* secure if no probabilistic polynomial time adversary A_I has non negligible advantage in winning the game. A_I is given access to all the six Oracles.

2.4 Game 2: Type 2 Adversary Confidentiality

A Certificateless Signcryption scheme(CLSC) is *IND-CLSC-CCA-2* secure if no probabilistic polynomial time adversary A_{II} has non negligible advantage in winning the game.

1. *Initialization:* Attacker A_{II} runs the *setup* algorithm and generates a master secret key s and the public system parameter *params*. A_{II} gives the secret s and *params* to C.
   Setup$(1^k) \rightarrow (Params, s)$

2. *Phase I Queries*
   Adversary A_{II} adaptively request the oracles with C: *Extract partial private key oracle, Request public key oracle, Signcryption oracle*
   A_{II} adaptively queries the oracle are alone used. It means the current query may depend on the previous query response. *Extract Partial Private Key Oracle* and *Replace Public Key Oracle* is not used.

3. *Challenge Stage:*
   Adversary A_{II} makes two messages of same length $\{m_0, m_1\}$ and two identities $\{ID_r, ID_s\}$. C randomly selects b $\in \{0,1\}$. Computes
   σ^* = *Signcrypt* (m_b, SK_s, PK_r)
   and sends σ^* to A_{II}.

4. *Guess Stage:* Adversary A_{II} is allowed to make a polynomial bounded number of queries like in Find Stage(). Adversary A outputs the guess b^1. If b^1 = b, then A_{II} wins the game. The following conditions hold:

   (a) Adversary A_{II} cannot get private key SK_{ID_r} for ID_r at any point.

   (b) Adversary A_{II} should not replace the receiver ID_r public key.

   (c) In the guess stage, Adversary A_{II} cannot make an *unsigncryption* query on σ^* under ID_{r^*}, ID_{s^*}.
   The advantage of A_{II} is defined as

$$Adv_{A_{II}}^{IND-CLSC-CCA-2} = \left|2Pr\left|b = b^1\right| - 1\right|$$

A certificateless signcryption scheme(CLSC) is *IND-CLSC-CCA-2* secure if no probabilistic polynomial time adversary A_{II} has non negligible advantage in winning the game.

2.5 Game 3: Unforgeability Type 1 Adversary

A Certificateless Signcryption scheme(CLSC) is said to be immune to existential forgery for adaptive chosen message

attacks *EUF-CLSC-CMA*, if no probabilistic polynomial time adversaries A_I and A_{II} have non negligible advantage in winning the game. This game is performed between the challenger and adversary A_I.

1.*Initialization:* Challenger C runs the *setup* algorithm and generates a master secret key s and the public system parameter *params*. Challenger C keeps s secret and sends *params* to A_I.
Setup$(1^k) \rightarrow (Params, s)$

2.*Phase I Queries:*
Adversary A_I request the Oracles with C: *Extract Partial Private Key Oracle, Request Public Key Oracle, Replace Public Key Oracle,Extract Private Key Oracle, Signcryption Oracle.* A_I adaptively queries the oracle. It means that the current query may depend on the previous query response.

3.*Forgery:*
A_I outputs a signcryption cipher text σ^* on message m^* two-challenge identities $\{ID_{r^*}, ID_{s^*}\}$ as receiver and sender respectively. A_I wins the *EUF-CLSC-CMA-1* game if σ^* is a valid signcryption with $\{ID_{r^*}, ID_{s^*}\}$ as receiver and sender respectively.
$m = UnSigncrypt\ (\sigma^*, ID_{r^*}, ID_{s^*})$
provided the following condition holds:

(a)σ^* is a not a output of any signcryption query on the message m with $\{ID_r, ID_s\}$ as receiver and sender respectively.
$\sigma^* = Signcrypt(m, ID_r, ID_s)$

(b)Adversary A_I cannot get private key SK_{ID_s} for ID_s at any point.

(c)Adversary A_I cannot obtain partial private key PSK_{ID_s} for ID_s, if the corresponding public key PK_{ID_r} has been replaced already during challenge phase.

(d)Adversary A_I cannot extract the private key for any identity if his / her public key has been replaced. The advantage of A_I is defined as

$$SUC_{A_I}^{EUF-CLSC-CMA} = \Pr\ |A_I wins|$$

2.6 Game 4: Unforgeability Type II Adversary

A Certificateless Signcryption scheme(CLSC) is said to be immune to existential forgery for adaptive chosen message attacks *EUF-CLSC-CMA*, if no probabilistic polynomial time adversary A_{II} has non negligible advantage in winning the game. This game is performed between the challenger and adversary A_{II}.

1.*Initialization:* Attacker A_{II} runs the *Setup* algorithm and generates a master secret key s and the public system parameter *params*. A_{II} gives the secret s and *params* to C.
Setup$(1^k) \rightarrow (Params, s)$

2.*Phase I Queries*
Adversary A_{II} adaptively request the oracles with C: *Extract Partial Private Key Oracle, Request Public Key Oracle, Signcryption Oracle*
A_{II} adaptively queries the oracle are alone used. It means the current query may depend on the previous query response. *Extract Partial Private Key Oracle* and *Replace Public Key Oracle* is not used.

3.*Forgery:*
A_{II} outputs a signcryption cipher text σ^* on message m^* two-challenge identities $\{ID_{r^*}, ID_{s^*}\}$ as receiver and sender respectively. A_{II} wins the *EUF-CLSC-CMA-1* game if σ^* is a valid signcryption with $\{ID_{r^*}, ID_{s^*}\}$ as receiver and sender respectively.
$m = UnSigncrypt\ (\sigma^*, ID_{r^*}, ID_{s^*})$
provided the following condition holds:

(a)σ^* is a not a output of any signcryption query on the message m with $\{ID_r, ID_s\}$ as receiver and sender respectively.
$\sigma^* = Signcrypt(m, ID_r, ID_s)$

(b)Adversary A_{II} cannot get private key SK_{ID_s} for ID_s at any point.
The advantage of A_{II} is defined as

$$SUC_{A_{II}}^{EUF-CLSC-CMA} = \Pr\ |A_I wins|$$

3 Proposed Scheme

With the rapid progress in mobile communication networks, smart devices and IoT devices, signcryption are under research and development stage. We propose our improved scheme which can be used in smart card environment [11]. The identities and messages are bit strings. The length of the bit strings is n_u and n_m respectively. The concept of the Internet of Things (IoT) and smart cards [6] have drawn considerable attention from both industry and academia. In the IoT, millions of objects with sensors collect data and send the data to servers that analyze, manage and use the data in order to construct some kinds of smart systems, such as smart grid, intelligent transportation systems, healthcare systems and even smart city. It is critical to establish a secure channel between the sensors and servers in order to ensure the correctness of collected data. Energy consumption and execution time is important in these resource constraint devices. If the collected data tampers, the results of data analysis are unbelievable, and may even bring serious disaster. The signcryption algorithm [12] is to be embedded on the microprocessor, which performs key generation, signcrypt and unsigncrypt

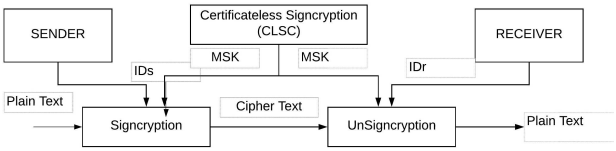

Fig. 2: Certificateless Signcryption Scheme

algorithms. The private keys are protected to read from external devices by the file structures of the operating system. The security goals that are required for smart card are non-repudiation, confidentiality and integrity. Signcryption scheme [13][14][15] achieves all the security requirements confidentiality, integrity, authentication, and nonrepudiation performing both the function of encryption and signing in one single logical step [16][17]. The current day smart card is having processor is of 32 or 16-bits. Cryptographic processor is used to perform cryptographic operations. All the information of users is stored in ROM during the manufacturing of cards. For the permanent store of data, EEPROM is used. Data is transferred either via the contacts on the cards surface or through electromagnetic fields in contact less card. The data can be accessed through a serial interface supervised by a security logic system and the operating system. The confidential data is in the ciphertext and can be processed internally by the chips arithmetic unit. It encourages the construction of several security mechanisms.

The scheme comprises of five algorithms, namely Master secret key generation for setup, Partial private key extraction, Random user key generation, Secret key Generation, and Signcrypt/Unsigncrypt.

3.1 Master Secret Key Generation

The setup phase provides security parameters 1^k as input and obtains master secret key msk. In addition the system parameters are also generated in this phase.
Input: Security parameter, User ID
Output: System parameters *params* and Master Secret Key *msk*.

1.*Setup:*

(a)The security parameter 1^k is given to Key Generation Center (KGC).

(b)KGC chooses G_1 and G_2 - cyclic group of prime order q.

(c)g - a random number generator.

(d)*e:* bilinear map : $G_1 \times G_1 \rightarrow G_T$

(e)Hash Function $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$

(f)It selects secret s, $s \in \mathbb{Z}_q^*$. It is used to construct the master secret key *msk*.
$msk = g^{s^2}$.

(g)Sets $g_1 = g^s$. It is the element in G_1 used in user key generation algorithm and in signcryption algorithm.

(h)n_u - Number of bits used in the identity *ID*

(i)u - element of g_1 used in the computation of $F_u(ID)$ - a function of identity and u used in computing partial private key and signcryption algorithm.

(j)υ - element of G_1 used in signcrypion algorithm.

(k)Select random vectors U and V. U = $(u_i) \in G_1$, V = $(v_j) \in G_1$

(l)Collision resistant Hash functions:
$H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$
$H_2 : \{0,1\}^* \rightarrow G_2 \rightarrow \mathbb{Z}_q^*$

The public parameters are $\{G_1, G_2, e, g, g_1, u, \upsilon, F_u, H_1, H_2\}$ and master secret key. $msk = g^{s^2}$.

3.2 Partial Private Key Generation

Once the master secret key msk is generated, and using user identity ID, the Key generation centre (KGC) generates a random number, the partial private key is generated using the below algorithm.

Input: Master Secret Key msk, User Id
Output: Partial private key

1.*Partial Private key Generator:* Given a user identity *ID*, the KGC randomly selects $r_{ID} \in \mathbb{Z}_q^*$ and computes partial private key as $PSK_{ID} = (PSK_{ID,1}, PSK_{ID,2})$
$PSK_{ID} = \left(g^{s^2} \times F_u(ID)^{r_{ID}}, g^{r_{ID}}\right)$

3.3 User Key Generation

The third step is the generation of user keys. The user identity *ID* and master secret key msk, are taken as input. Secret value X_{ID} is generated for user identity *ID* and PK_{ID} is obtained as output.
Input: Master Secret Key msk, User *ID*
Output: Secret value X_{ID}, Partial private key PK_{ID}.

The user *ID* randomly selects $x_{ID} \in \mathbb{Z}_q^*$ as his secret value.

$PK_{ID} = (PK_{ID,1}, PK_{ID,2})$
$PK_{ID} = \left(g_1^{x_{ID}}, v^{\frac{1}{x_{ID}}}\right)$

3.4 Secret Key Generation

The user identity ID and master secret key msk, are taken as input. Secret value X_{ID} is generated for user identity ID and PK_{ID} is obtained as output.
Input: Master Secret Key msk, User ID
Output: Secret private key SK_{ID}.

The user ID sets his private key SK_{ID}
$SK_{ID} = (SK_{ID,1}, SK_{ID,2}, SK_{ID,3})$
$SK_{ID} = (PSK_{ID,1}, PSK_{ID,2}, x_{ID})$

3.5 Signcryption

After successful generation of keys, signcryption is performed by the sender, and the unsigncrypt is performed on the receiving end by the receiver. The input to the signcryption function includes, the system parameters *params*, message m, sender with identity ID_s, receiver with identity ID_r, senders private key SK_{ID_s}, and receivers public key PK_{ID_r}. The output of the signcrypt() function is the cipher text σ.

Similarly at the receiving end, the receiver performs the unsigncrypt() function. The input to this function is the system parameters, cipher text σ, sender with identity ID_s, receiver with identity ID_r, senders public key PK_{ID_s}, and receivers private key SK_{ID_r}. The output of the unsigncrypt() function is the plain text or original message m.

Suppose the sender with identity ID_s wants to send message $m \in G_2$ to the receiver with identity ID_r.

1.Checks the public key of the receiver
$e\,(PK_{r,1}, PK_{r,2}) = e\,(g_1, v)$

2.Select random values $r_1, r_2 \in \mathbb{Z}_q^*$

3.Computes

(a)$\sigma_1 = H_2\,(m \parallel \mathbb{T}) \times e\,(PK_{r,1}, PK_{r,2})^{r_1} \times e\,(g_1, g_1)^{r_2}$
$\mathbb{T} \in \{0,1\}^*$

(b)$\sigma_2 = e\,(g_1, g_1)^{r_1}$

(c)$\sigma_3 = g^{r_2}$

(d)$\sigma_4 = F_u(ID)^{r_2}$

(e)$\sigma_5 = SK_{s,2}^{SK_{s,3}^2}$

(f)$w =$
$H_1\,(T, ID_s, ID_r, PK_{s,1}, PK_{s,2}, PK_{r,1}, PK_{r,2}, \sigma_*)$
where $\sigma_* = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$

(g)$\sigma_6 = SK_{s,2}^{SK_{s,3}^2} \times v^{r_{2,w}}$

The Signcryption ciphertext is
$\sigma = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$

3.6 UnSigncryption

1.The receiver R verifies the senders public key PK_{ID}.
$e\,(PK_{r,1}, PK_{r,2}) = e\,(g, v)$

2.R computes $H_2^{-1}\left[\sigma_1 \times \dfrac{e\,(SK_{r,2}, \sigma_4)}{e\,(\sigma_3, SK_{r,1}) \times \sigma_2^{SK_{r,3}^2}}\right]$

3.$w =$
$H_1\,(T, ID_s, ID_r, PK_{s,1}, PK_{s,2}, PK_{r,1}, PK_{r,2}, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$
and verifies
$e\,(\sigma_6, g) =$
$e\,(PK_{s,1}, PK_{s,1}) \times e\,(F_u(ID_s), \sigma_5) \times e\,(v^w, \sigma_3)$
Then it accepts the message.

3.7 Correctness of the algorithm

1.$e\,(\sigma_6, g) = e\left(SK_{s,1}^{SK_{s,3}^2}.v^{r_{2,w}}, g\right)$

2.$e\,(\sigma_6, g) = e\left(g^{s^2 \times x_s^2}.F_u(ID_s)^{x_s^2 . r_2}, g\right).e\,(v^{r_{2,w}}, g)$

3.$e\,(\sigma_6, g) =$
$e\,(PK_{s,1}, PK_{s,1}).e\left(F_u(ID_s), g^{s^2}\right).e\,(v^w, \sigma_3)$
$e\,(\sigma_6, g) =$
$e\,(PK_{s,1}, PK_{s,1}) \times e\,(F_u(ID_s), \sigma_5) \times e\,(v^w, \sigma_3)$

4.where $\sigma_6 = SK_{s,1}^{SK_{s,3}^2}.v^{r_{2,w}}$

5.$SK_{ID} = (SK_{ID,1}, SK_{ID,2}, SK_{ID,3})$
$SK_{ID} = (PSK_{ID,1}, PSK_{ID,2}, x_{ID})$

6.$PK_{ID} = (PK_{ID,1}, PK_{ID,2})$
$PK_{ID} = \left(g_1^{x_{ID}}, PK_{ID,2}, v^{\frac{1}{x_{ID}}}\right)$

7.$\sigma_5 = g^{x_s^2}$

4 Conclusion

In this paper, we have proposed a new certificateless signcryption scheme and proved its security. The

proposed scheme is robust against all proposed attacks. The proposed scheme is semantically secure against adaptive chosen ciphertext attack. It is also secure against existential unforgeability against adaptive chosen message attack. Since our scheme does not require many multiplication operation, and this characteristic makes our scheme very suitable for resource-constrained devices. This scheme has an application to ensure data integrity in the Internet of Things based on cloud environment. The Internet of Things (IoT) is an emerging network paradigm that aims to obtain the interactions among pervasive things through heterogeneous networks. Security is an important task in the IoT, for which the security can be achieved by using our proposed technique.

Acknowledgement

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, Proceedings of CRYPTO '84 on Advances in Cryptology, LNCS 196, pp. 47-53, Springer-Verlag (1985).
[2] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Advances in Cryptology CRYPTO 2001,Lecture Notes in Computer Science, Vol. 2139. pp. 213-229,Springer, Berlin, Heidelberg (2001).
[3] J. Malone-Lee, Identity-Based Signcryption, Cryptology ePrint Archive, (2002).
[4] S.S. Al-Riyami and K.G. Paterson, Certificateless Public-Key Cryptography, Advances in Cryptology ASIACRYPT 2003, LNCS Vol. 2894 pp. 452-473. Springer-Verlag (2003).
[5] Y. Zheng, Digital Signcryption or How to Achieve Cost(Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption). Advances in Cryptology CRYPTO 97, LNCS 1294, pp. 165-179, Springer-Verlag (1997).
[6] M. Barbosa and P. Farshim, Certificateless signcryption, Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, pp. 369-372 (2008).
[7] Z. Liu, Y. Hu, X. Zhang and H. Ma, Certificateless signcryption scheme in the standard model, Information Sciences, Vol.180, No. 3, pp. 452-464 (2010).
[8] Y. Yuan and C. Wang, A Secure Certificateless Signature Scheme in the Standard Model, Journal of Computational Information Systems, Vol.11, No. 9, pp. 4353-4362 (2013).
[9] Xu, Z, Dai G. and Yang D, An efficient online/offline signcryption scheme for MANET, Advanced Information Networking and Applications Workshops-AINAW 2007, pp. 171-176 (2007).
[10] F. Yan, X. Chen and Y. Zhang, Efficient online/offline signcryption without key exposure, International Journal of Grid and Utility Computing, Vol. 4, No. 1, pp. 85-93, (2013).
[11] D. Sun, X. Huang, Y. Mu, and W. Susilo, Identity-based on-line/off-line signcryption, Proceedings of IFIP International Conference on Network and Parallel Computing, pp. 3441 (2008).
[12] K.A. Shim, CPAS An efficient conditional privacy preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology, Vol. 61, No. 4, pp. 18741883 (2012).
[13] L. Cheng and Q. Wen, An Improved Certificateless Signcryption in the Standard Model, International Journal of Network Security, vol 17, No. 5, pp. 597-606 (2015).
[14] J.C. Cha, and J.H. Cheon, An identity-based signature from gap Diffie-Hellman groups, Public Key Cryptography PKC 2003, LNCS 2567, pp. 1830 (2003).
[15] M. Luo, M. Tu and J. Xu, A security communication model based on certificateless online/offline signcryption for Internet of Things. J Security and Communication Networks, Vol. 7, No. 10, pp. 15601569 (2014).
[16] J. Weng, G. X. Yao, R. H. Deng, M. R. Chen, and X. X. Li, Cryptanalysis of a certificateless signcryption scheme in the standard model, J Information Sciences, Vol. 181, No. 3, pp. 661-667 (2011).
[17] S. Miao, F. Zhang, S. S. Li, and Y. Mu, On security of a certificateless signcryption scheme, J Information Sciences, Vol. 232, pp. 475-481 (2013).

Balasubramanian.V is an Assistant Professor in Computer Science and Engineering, SSN College of Engineering, Chennai, received his Masters degree in Computer Science and Engineering from Anna University. He is currently pursuing Ph.D. degree in the Department of Information Science and Technology, Anna University, Chennai, India. His research interest includes Cryptography and Data Security in Cloud Services. He is a member of ISTE, CSI, IEEE and ACM.

Mala Thangarathinam is an Associate Professor in the Department of Information Science and Technology, Anna University, India. She completed her Ph.D. on NLP at Anna University during the year 2008. Currently, she is guiding more than ten research scholars. Her research areas include natural language processing, virtualization technologies, grid computing and cloud computing. She has more than 10 research publications in national conferences, 20 research publications in international conferences and 12 research publications in international journals.